Departamento de Matemática da Universidade de Coimbra
Teoria dos Números

Uma possível resolução do 2^o Teste — Prova A

11 de Dezembro de 2003 — Duração: 30m

---

1. (0,3 valores)
Resolva a congruência $10x \equiv 6 \pmod{14}$.

Uma vez que $(10, 14) = 2$ e $2 \mid 6$, a congruência dada tem duas soluções, isto é, existem duas classes de congruência módulo 14 cujos elementos verificam a congruência dada. Determinem-se essas duas classes.

$$10x \equiv 6 \pmod{14} \Leftrightarrow 2 \times 5x \equiv 2 \times 3 \pmod{2 \times 7} \Leftrightarrow 5x \equiv 3 \pmod{7}.$$

Use-se o Algoritmo de Euclides para escrever $1 = (5, 7)$ como soma de múltiplos de 5 e 7. $7 = 1 \times 5 + 2$ e $5 = 2 \times 2 + 1$. Assim, $1 = 5 - 2 \times 2 = 5 - 2 \times (7 - 5) = (-2) \times 7 + 3 \times 5$ e portanto $5 \times 3 \equiv 1 \pmod{7}$. Então $5 \times 9 \equiv 3 \pmod{7}$ e os inteiros que satisfazem a congruência dada são todos os inteiros pertencentes a $[9]_7 = [2]_7$. Esta classe de congruência módulo 7 é união de duas classes de congruência módulo 14, a saber, $[2]_{14}$ e $[2 + 7]_{14} = [9]_{14}$.

---

2. (0,3 valores)
Sejam $\mathbf{n} \in \mathbb{N}$, $\mathbf{a} \in \mathbb{Z}$ ímpar e tal que $(\mathbf{a}, \mathbf{5}) = \mathbf{1}$. Determine o último dígito de $\mathbf{a^{8n} + 1}$.

O último dígito de $a^{8n} + 1$ é o elemento do sistema completo de resíduos módulo 10, $\{0, 1, \ldots, 9\}$, com o qual $a^{8n} + 1$ é congruente módulo 10. Sendo a ímpar, $(a, 2) = 1$. Como também $(a, 5) = 1$, conclui-se que $(a, 10) = 1$. Assim, o teorema de Euler garante que $a^{\varphi(10)} \equiv 1 \pmod{10}$. Uma vez que 2 e 5 são primos, $\varphi(10) = \varphi(2 \times 5) = (2^1 - 2^0)(5^1 - 5^0) = (2 - 1)(5 - 1) = 4$ e portanto $a^4 \equiv 1 \pmod{10}$. Então

$$a^{8n} + 1 = \left(a^4\right)^{2n} + 1 \equiv 1^{2n} + 1 \pmod{10} \equiv 2 \pmod{10}$$

e o último dígito de $a^{8n} + 1$ é 2.

---

3. (0,4 valores)
Prove que, para todo o $\mathbf{n} \in \mathbb{N}$, se tem $\varphi(\mathbf{n^2}) = \mathbf{n}\, \varphi(\mathbf{n})$.

Seja $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ a decomposição canónica de n, isto é, $r \in \mathbb{N}$, $p_1, p_2, \ldots, p_r$ são números primos distintos dois a dois e $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}$. Então

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdots \left(p_r^{\alpha_r} - p_r^{\alpha_r - 1}\right).$$

A decomposição canónica de n^2 é $p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_r^{2\alpha_r}$ e portanto

$$\begin{aligned}
\varphi\left(n^2\right) &= \left(p_1^{2\alpha_1} - p_1^{2\alpha_1-1}\right)\left(p_2^{2\alpha_2} - p_2^{2\alpha_2-1}\right)\cdots\left(p_r^{2\alpha_r} - p_r^{2\alpha_r-1}\right) \\
&= p_1^{\alpha_1}\left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right) p_2^{\alpha_2}\left(p_2^{\alpha_2} - p_2^{\alpha_2-1}\right)\cdots p_r^{\alpha_r}\left(p_r^{\alpha_r} - p_r^{\alpha_r-1}\right) \\
&= \left(p_1^{\alpha_1} p_2^{\alpha_2}\cdots p_r^{\alpha_r}\right)\left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2-1}\right)\cdots\left(p_r^{\alpha_r} - p_r^{\alpha_r-1}\right) \\
&= n\,\varphi(n)\,.
\end{aligned}$$